Tle

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/648,628	08/25/2003	Chun Kin Chan	CHAN 1-4-2-4-2-8. (LCNT/12	4361

46363 7590 06/28/2007
PATTERSON & SHERIDAN, LLP/
LUCENT TECHNOLOGIES, INC
595 SHREWSBURY AVENUE
SHREWSBURY, NJ 07702

EXAMINER	
SCHELL, JOSEPH O	
ART UNIT	PAPER NUMBER
2114	
MAIL DATE	DELIVERY MODE
06/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/648,628	**Applicant(s)** CHAN ET AL.
	Examiner Joseph Schell	**Art Unit** 2114

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 November 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19,24-28 and 34* is/are rejected.

7)☒ Claim(s) *20-23 and 29-33* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Detailed Action

Claims 1-34 have been examined.

Claims 20-23 and 29-33 have been objected to as containing allowable subject matter, yet dependant upon rejected base claims.

Claims 1-19, 24-28 and 34 have been rejected.

Claim Objections

1. Claims 4, 17 and 26 are objected to.

Claim 4 line 3 should read "instance where said network degradation event" to avoid confusing it with brink of failure events.

Claim 4 lines 4-5 state "to affect at least one of a critically defined network functionality". This use of "at least one of" implies that the phrase will be followed by an enumeration of a group having more than one element. The examiner recommends removing "of a" from this limitation.

Claim 4 line 5 states the limitation "critically defined network functionality". This use of "critically defined" is improper as it implies that the act of defining was performed in a critical manner. The examiner recommends replacing the limitation with "critical network functionality" to limit the network functionalities to those that are critical.

Claim 17 (lines 11 and 12-13) and Claim 26 (lines 3 and 4-5) are objected to for the same reasons as discussed above with respect to Claim 4.

Allowable Subject Matter

2. Claims 20-23 and 29-33 are objected to as containing novel subject matter yet being dependent on rejected base claims.

Claims 9-13 and 15-16 contain novel subject matter yet are rejected under 35 U.S.C. 112, as detailed below.

Within claims 9, 20 and 29, the examiner deems the novel limitation to be, within the entirety of each claim, the determination of whether a Breach-of-Security event caused by a Brink-of-Failure event also causes a Brink-of-Failure event.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 8-13, 15-16, 22, and 31 are rejected under 35 U.S.C. 112 second paragraph as being indefinite.

4. Claim 8 line 3 states the limitation "said existing conditions database". This limitation lacks antecedent basis within the claim.

Claim 8 line 4 states the limitation "said network topology database". This limitation lacks antecedent basis within the claim.

5. Within Claims 12, 22 and 31, within the first two lines of each claim it is stated that the limitations of the claim are applicable only when the network degradation event is a breach-of-security event. These claims are potentially non-limiting. Additionally, with respect to claim 31, it is indefinite how an apparatus can further comprise means for additional functions *only* when an event is classified as a breach-of-security.

6. Claim 17 lines 9-10 recites "defining said.. event.. in an instance where said event is at least one of..." and is rejected as containing indefinite limitations, as discussed above.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-3, 14, 24-25, and 34 are rejected under 35 U.S.C. 102(e) as being anticipated by Roletto (US Patent Application Publication 2004/0221190).

8. As per claim 1, Roletto ('190) discloses a method for managing a network, comprising the steps of:

detecting occurrence of a network event, said network event having associated with it a network condition comprising at least one of an unplanned macro-event (paragraph 10) and a planned macro-event related to at least one of a network element and a communication link of said network;

classifying said network event as being at least one of a network element failure, a communications link failure, and a security breach (paragraph 53); and

identifying said network event as a network degradation event in response to at least one network event exceeding a network degradation threshold (paragraph 84, denial of service attacks are identified by incoming packet counts).

9. As per claim 2, Roletto ('190) discloses the method of claim 1, further comprising the step of: sending an alert to normalize said network degradation event (end of paragraph 78, events may be sorted by severity, this requires normalization because there are different kinds of events (see paragraph 73). Thus a threshold-surpassing number of packets that determine a denial-of-service attack may be greater than the number of packets identifying a router failure, for example, while the severity of the event is not necessarily greater).

10. As per claim 3, Roletto ('190) discloses the method of claim 1, wherein said network event is associated with at least one of a network management system, a security management system (see abstract), and a system timer.

11. As per claim 14, Roletto ('190) discloses the method of claim 1, wherein said step of identifying a network event comprises the step of identifying events associated with at least one of end-user data traffic (paragraph 10), in-band control traffic, out-of-band control traffic, in-band network management traffic, and out-of-band network management traffic.

12. As per claims 24-25, these claims recite limitations found in claims 1-2 and are rejected on the same grounds,as claims 102.

13. As per claim 34, this claim recites limitations found in claim 1 and is rejected on the same grounds as claim 1.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 4, 7, 17-18, 26 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roletto ('190) in view of Berg (US Patent 5,872,911).

15. As per claim 4, Roletto ('190) discloses the method of claim 1.

Roletto ('190) discloses the use of packet-count variance calculations (paragraph 83) and packet-count hard limits (paragraph 84) to determine the severity of events. Roletto ('190) additionally discloses the defining of a brink of failure event when said network event affects a critically defined network functionality (paragraph 80, denial of service attacks target servers).

Roletto ('190) does not expressly disclose the method, wherein said step of identifying comprises the step of: defining said network degradation event as a brink of failure (BOF) event in an instance where said event is at least one of a type determined to cause a failure of at least one network element within a predetermined time interval, and to affect a number of end users exceeding a predetermined threshold level.

Berg ('911) teaches a system that analyzes failures in a network, filtering them according to their severity, wherein the severity is dependent on imminence of the failure and the number of customers affected (column 3 line 60 through column 4 line 1).

At the time of invention it would have been obvious to a person of ordinary skill in the art to modify the security failure analysis system disclosed by Roletto ('190) such that the severity of events is additionally based on the imminence of a failure due to a denial-of-service attack and the users affected by such a failure. This modification would have been obvious because the use of such information provides for improved service availability with limited human resources (Berg ('911) column 3 lines 1-10).

16. As per claim 7, Roletto ('190) in view of Berg ('911) discloses the method of claim 4, wherein said step of identifying further comprises the step of:

defining said network degradation event as a breach-of-security (BOS) event in an instance where said network event exploits a security vulnerability resulting in at least one of an unauthorized access (Roletto ('190) paragraph 80), an unauthorized modification or compromise, a denial of access to information, a denial of access to network monitoring capability, and a denial of access to network control capability.

17. As per claim 17, Roletto ('190) discloses a method for managing a network, comprising the steps of:

detecting occurrence of a network event, said network event having associated with it a network condition comprising at least one of an unplanned macro-event (paragraph 10) and a planned macro-event related to at least one of a network element and a communication link of said network;

classifying said network event as being at least one of a network element failure, a communications link failure, and a security breach (paragraph 53);

identifying said network event as a network degradation event in response to at least one network event exceeding a network degradation threshold (paragraph 84, denial of service attacks are identified by incoming packet counts) by defining said network degradation event as a brink of failure (BOF) event in an instance where said event is to affect at least one of a critically defined network functionality (paragraph 80, denial of service attacks target servers); and

sending an alert to normalize said network degradation event (end of paragraph 78, events may be sorted by severity, this requires normalization because there are different kinds of events (see paragraph 73). Thus a threshold-surpassing number of packets that determine a denial-of-service attack may be greater than the number of packets identifying a router failure, for example, while the severity of the event is not necessarily greater).

Roletto ('190) does not expressly disclose the method, wherein said step of identifying comprises the step of: defining said network degradation event as a brink of failure (BOF) event in an instance where said event is at least one of a type determined to cause a failure of at least one network element within a predetermined time interval, and to affect a number of end users exceeding a predetermined threshold level.

Berg ('911) teaches a system that analyzes failures in a network, filtering them according to their severity, wherein the severity is dependent on imminence of the failure and the number of customers affected (column 3 line 60 through column 4 line 1).

At the time of invention it would have been obvious to a person of ordinary skill in the art to modify the security failure analysis system disclosed by Roletto ('190) such that the severity of events is additionally based on the imminence of a failure due to a denial-of-service attack and the users affected by such a failure. This modification would have been obvious because the use of such information provides for improved server availability with limited human resources (Berg ('911) column 3 lines 1-10).

18. As per claim 18, this claim recites limitations found in claim 7 and is rejected on the same grounds as claim 7.

19. As per claim 26, this claim recites limitations found in claim 4 and is rejected on the same grounds as claim 4.

20. As per claim 27, this claim recites limitations found in claim 7 and is rejected on the same grounds as claim 7.

21. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Roletto ('190) in view of Guibellot (US Patent 7,024,580).

Roletto ('190) discloses the method of claim 5. Roletto ('190) does not expressly disclose the method wherein said step of identifying said network degradation event comprises the step of:

assessing at least one of failure rates, mean-time-between-failures (MTBF), mean-time-to-repair (MTTR), and spare parts availability for at least one of network elements and communication links associated with said network event.

Guibellot ('580) teaches calculating the availability of a cluster system using mean time to fail and mean time to repair.

At the time of invention it would have been obvious to a person of ordinary skill in the art to modify the security failure analysis system disclosed by Roletto ('190) such that mean time to repair data is assessed when determining the severity of a network failure. This modification would have been obvious because knowledge of the mean time a system takes when transition from active to failed to fail-over allows for an accurate determination of the system's average availability (see Guibellot ('580) column 2 lines 30-40), while system availability knowledge is useful for contract planning (Guibellot ('580) column 1 lines 35-45).

22. Claims 6 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roletto ('190) in view of Dev (US Patent 5,261,044).

23. As per claim 6, Roletto ('190) discloses the method of claim 1. Roletto ('190) does not expressly disclose the method wherein in response to the step of classifying said network event, said method further comprises the steps of:

updating an existing conditions database with indicia of said network event;
determining a latest network topology associated with said network event; and
updating a network topology database with said latest network topology.

Dev ('044) teaches the use of a network map displaying the status of network nodes and links (see abstract).

At the time of invention it would have been obvious to a person of ordinary skill in the art to modify the security failure analysis system disclosed by Roletto ('190) such that it employs a network map to display network status information. This modification would have been obvious because such a map presents the information in a clear and well-organized display (Dev ('044) column 2 lines 20-24).

24. As per claim 28, this claim recites limitations found in claim 6 and is rejected on the same grounds as claim 6.

25. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Roletto ('190) in view of Berg ('911) and in further view of Guibellot ('590) and Dev ('044).

Roletto ('190) in view of Berg ('911) discloses the method of claim 7. Roletto ('190) in view of Berg ('911) does not expressly disclose the method wherein said step of defining said network degradation event as a brink-of-failure (BOF) event further comprises the step of: correlating network events stored in said existing conditions database with information stored in said network topology database and events stored in a scheduled events database.

Guibellot ('580) teaches calculating the availability of a cluster system using mean time to fail and mean time to repair (see abstract). This allows for prediction of failures and scheduling of anticipated failure events.

At the time of invention it would have been obvious to a person of ordinary skill in the art to modify the security failure analysis system disclosed by Roletto ('190) such that mean time to repair data is assessed when determining the severity of a network failure. This modification would have been obvious because knowledge of the mean time a system takes when transition from active to failed to fail-over allows for an accurate determination of the system's average availability (see Guibellot ('580) column 2 lines 30-40), while system availability knowledge is useful for contract planning (Guibellot ('580) column 1 lines 35-45).

Dev ('044) teaches the use of a network map displaying the status of network nodes and links (see abstract).

At the time of invention it would have been obvious to a person of ordinary skill in the art to modify the security failure analysis system disclosed by Roletto ('190) such that it employs a network map to display network status information. This modification would have been obvious because such a map presents the information in a clear and well-organized display (Dev ('044) column 2 lines 20-24).

26. Claims 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Roletto ('190) in view of Berg ('911) and in further view of Dev ('044).

Roletto ('190) in view of Berg ('911) discloses the method of claim 18. Roletto ('190) in view of Berg ('911) does not expressly disclose he method wherein in response to the step of classifying said network event, said method further comprises the steps of:

> updating an existing conditions database with indicia of said network event;
>
> determining a latest network topology associated with said network event; and
>
> updating a network topology database with said latest network topology.

Dev ('044) teaches the use of a network map displaying the status of network nodes and links (see abstract).

At the time of invention it would have been obvious to a person of ordinary skill in the art to modify the security failure analysis system disclosed by Roletto ('190) such that it employs a network map to display network status information. This modification would have been obvious because such a map presents the information in a clear and well-organized display (Dev ('044) column 2 lines 20-24).

Conclusion

The prior art made of record on accompanying PTO 892 form and not relied upon is considered pertinent to applicant's disclosure. Specifically, Smith ('102) teaches classifying devices in a SAN according to their impending-failure status for predictive maintenance, and Cox ('335) and Shirakawa ('247) teach networks wherein a central controller performs monitoring and failure predictions for the nodes.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Schell whose telephone number is (571) 272-8186. The examiner can normally be reached on Monday through Friday 9AM-4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Scott Baderman can be reached on (571) 272-3644. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JS

SCOTT BADERMAN
SUPERVISORY PATENT EXAMINER